

IN THE CLAIMS:

1. (Previously Presented) A method for filtering incoming data from an external computer network, comprising:

a firewall that is coupled to said external computer network;

a server computer system coupled to an internal computer network;

a plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly;

receiving, at said firewall, a document from said external computer network;

determining, by said firewall, whether said document is from a known blocked site;

in response to determining that said document is from a known blocked site, blocking, by said firewall, said document without scanning said document;

determining, by said firewall, whether said document is from a known safe site;

in response to determining that said document is from a known safe site, forwarding, by said firewall, said document to said server without scanning said document, all of said plurality of clients being permitted to access said forwarded document;

in response to determining that said document is not from a known blocked site or a known safe site, scanning, by said firewall, text fields included in said document for pre-selected keyword(s);

blocking, by said firewall, the document if any of said text fields include content that contains pre-selected keywords;

said server computer system being prohibited from receiving said document in response to said document being blocked; and

indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of said site to a filtering table.

2. (Canceled)

3. (Previously Presented) The method according to claim 1, wherein the document is allowed to pass per standard service rules if the content does not contain pre-selected keyword(s).

4. (Previously Presented) The method according to claim 1, further comprising storing an indication in said filtering table of each known safe site that can be passed per standard service rules without having to be scanned for pre-selected keywords.
5. (Previously Presented) The method according to claim 1, wherein the step of indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of a site to a filtering table further comprises adding the address of the site to a "known-block" table when said site has sent a document that includes said pre-selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords.
6. (Original) The method according to claim 1, wherein the addition of a site to the filtering table is implemented using a strong text parsing language.
7. (Currently amended) The method according to claim 1, wherein the instance of the filter is periodically refreshed ~~through a timed job on a Windows NT platform, a cron job on a UNIX platform,~~ to enact the updated filtering tables.
8. (Previously Presented) A computer program product in a computer readable medium for use in a data processing system for filtering incoming data from an external computer network, the computer program product comprising:
 - a firewall that is coupled to said external computer network;
 - a server computer system coupled to an internal computer network;
 - a plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly;
 - instructions for receiving, at said firewall, a document from said external computer network;
 - instructions for determining, by said firewall, whether said document is from a known blocked site;
 - in response to determining that said document is from a known blocked site, instructions for blocking said document without scanning said document;

instructions for determining, by said firewall, whether said document is from a known safe site;

in response to determining that said document is from a known safe site, instructions for forwarding said document to said server without scanning said document, all of said plurality of clients being permitted to access said forwarded document;

in response to determining that said document is not from a known blocked site or a known safe site, instructions for scanning, by said firewall, text fields included in said document for pre-selected keyword(s);

instructions for blocking, by said firewall, the document if any of said text fields include content that contains pre-selected keywords;

said server computer system being prohibited from receiving said document in response to said document being blocked; and

instructions for indicating that a site that sent said document is a known blocked site by adding, by said firewall, the address of said site to a filtering table.

9. (Canceled)

10. (Previously Presented) The computer program product according to claim 8, further comprising instructions for allowing the document to pass per standard service rules if the content does not contain pre-selected keyword(s).

11. (Previously Presented) The computer program product according to claim 8, further comprising instructions for storing an indication in said filtering table of each known safe site that can be passed per standard service rules without having to be scanned for pre-selected keywords.

12. (Previously Presented) The computer program product according to claim 8, wherein the instructions for indicating that a site that sent said document is a known blocked site by adding, by said firewall, that address of said site to a filtering table further comprises adding the address of said site to a "known-block" table when said site has sent a document that includes said pre-

selected keywords so that the site will be blocked in the future without having its contents scanned for pre-selected keywords.

13. (Original) The computer program product according to claim 8, wherein the instructions for addition of a site to the filtering table are implemented in a strong text parsing language.

14. (Currently amended) The computer program product according to claim 8, wherein the instance of the filter is periodically refreshed ~~through a timed job on a Windows NT platform, a cron job on a UNIX platform,~~ to enact the updated filtering tables.

15. (Previously Presented) A system for filtering incoming data from an external computer network, the system comprising:

- a firewall that is coupled to said external computer network;
- a server computer system coupled to an internal computer network;
- a plurality of clients that are coupled to said server computer system, said plurality of clients being unable to access said external computer network directly;
- said firewall for receiving a document from said external computer network;
- said firewall for determining whether said document is from a known blocked site;
- in response to determining that said document is from a known blocked site, said firewall for blocking said document without scanning said document;
- said firewall for determining whether said document is from a known safe site;
- in response to determining that said document is from a known safe site, said firewall for forwarding said document to said server without scanning said document, all of said plurality of clients being permitted to access said forwarded document;
- in response to determining that said document is not from a known blocked site or a known safe site, said firewall for scanning text fields included in said document for pre-selected keyword(s);
- said firewall for blocking the document if any of said text fields include content that contains pre-selected keywords;
- said server computer system being prohibited from receiving said document in response to said document being blocked; and

said firewall for indicating that a site that sent said document is a known blocked site by adding the address of said site to a filtering table.